AGENCY FOR DIGITAL GOVERNMENT

Den Danske Stat
OCES2 vs OCES3

 Version date: 20-03-2023
 Version: 1.1
 Page 1 of 12

OCES2 vs OCES3

Contents

1	I	ntroduct	ion	3
	1.1	Inte	nded audience	3
2	ľ	MOCES ('	"employee certificates")	4
	2.1	Cert	ificate content	4
	2	2.1.1	Formalia	4
	2	2.1.2	Distinguished Name	4
	2	2.1.3	Extensions	5
3	١	/OCES (o	organizational certificates)	7
	3.1	Cert	ificate content	7
	3	3.1.1	Formalia	7
	3	3.1.2	Distinguished Name	7
	3	3.1.3	Extensions	8
4	F	OCES (F	unctional certificates)	9
	4.1	Cert	ificate content	9
	2	1.1.1	Formalia	9
	2	1.1.2	Distinguished Name	9
	2	1.1.3	Extensions	10
5	(CRL		11
	5.1	CRL	content	11
	5	5.1.1	Formalia	11
	5	5.1.2	Extensions	11
6	ľ	More info	ormation	12

1 Introduction

This document compares the structure of a OCES2 (Nets/NemID) certificate with the structure of a OCES3 (Den Danske Stat/MitID Erhverv) certificate. The new structure of OCES3 certificates is different from the existing OCES2 certificates and more compliant with European standards¹ on certificate content. OCES2 was developed before the European standards were developed and settled and did therefore not match the evolving standards.

Note that this document does not elaborate on qualified certificates, which is also part of the MitID Erhverv infrastructure.

Note also that personal OCES certificates are discontinued in the new infrastructure and replaced with qualified certificates.

This document does not describe the implemented services related to the certificate issuance and management like the fact that partial certificate revocation lists via LDAP is not supported in the new infrastructure.

1.1 Intended audience

The intended reader is a technical person, which are familiar with X.509 certificates and is responsible of adjusting existing applications using OCES2 certificates.

 Version date: 20-03-2023
 Version: 1.1
 Page 3 of 12

¹ ETSI EN 319 412-1, ETSI EN 319 412-2 and ETSI EN 319 412-5.

2 MOCES ("employee certificates")

2.1 Certificate content

2.1.1 Formalia

Field	MOCES2 (employee-cert)	MOCES3 (user-cert)	Remarks
X.509 version	3	3	No change ²
SerialNumber			No change
Validity Period			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with	RSASSA-PSS with SHA-	
	SHA-256	256 ³	
Trust anchor	TRUST2408	Den Danske Stat OCES	
		rod-CA	
Public key	2048 bits RSA key	3072 bits RSA key	

2.1.2 Distinguished Name

Field	MOCES2	MOCES3	Remarks
country	DK	DK	No change
organizationName	Certificate subscribers organizational name and CVR number (UTF8String) in the form "OrgName // CVR:xxxxxxxx" where the OrgName is the registered name of the organization and xxxxxxxxx is the CVR number	Certificate subscribers organizational name	The separator ' // ' and the CVR-number is not included in organizational name in MOCES3. For MOCES3 the CVR can be found in organisationIdentifier
organizationalUnit	Optional	No supported	
commonName	Certificate subjects name which may include the title e.g. "CEO John Doe"	Certificate subject's name or pseudonym	
givenName	N/A	Certificate subject's given name SHALL be present if surname is present. MUST not be present if pseudonym is present.	
surname	N/A	Certificate subject's surname SHALL be present if givenName is present. MUST not be present if pseudonym is present.	
pseudonym	N/A	Certificate subject's pseudonym	

 $^{^{\}rm 2}$ Note that ASN.1-wise this value is encoded as the value 2 since X.509 enumerates from 0.

 $^{^{\}rm 3}$ Note that CA certificates are using SHA-512

Version date: 20-03-2023	Version: 1.1	Page 4 of 12
--------------------------	--------------	--------------

		MUST not be present if		
		givenName and surname		
		is present.		
organizationIdentifier	N/A	Certificate subscriber's		
		CVR-number in the form		
		NTRDK-XXXXXXXX where		
		XXXXXXXX is the CVR-		
		number of the		
		organization.		
serialNumber	Unique identifier for the	Unique identifier for the	Note that the X's in the	
	certificate subject in the	certificate subject in the	MOCES3 is NOT the	
	form CVR:XXXXXXXX	form UI:DK-	certificate subjects	
	RID:XXXX	X:X:XXXXXXXXX	RID-number.	
	Migrating from RID to UUID is supported by the supporting services API			
https://tu.nemlog-in.dk/oprettelse-og-administration-af-tjeneste			nf-tjenester/log-	
	in/hjaelp-og-vejledning/			

2.1.3 Extensions

Field	MOCES2	MOCES3	Remarks
keyUsage	digitalSignature,	digitalSignature,	MOCES3 use
	contentCommitment,	contentCommitment,	profile F of ETSI
	keyEncipherment,	keyEncipherment	EN 319 412-2
	dataEncipherment,		section 4.3.2
	keyAgreement		
certificatePolicies	OID reference to	OID references to MOCES3	The link to
	MOCES2 policies +	policies +	repository and
	Link to repository +	OID reference to the	the user notice is
	User notice	compliant NCP policy	discontinued
	referencing the		
	underlying policy.		
cRLDistributionPoints	HTTP link to CRL +	HTTP link to CRL	LDAP path to a
	LDAP path to a partial		partial CRL is
	CRL		discontinued.
			Full CRL or OCSP
			should be used
			as an alternative.
accessInformationAuthority	Reference to OCSP	Reference to OCSP	No change
	responder +	responder +	
	Reference to the	Reference to the certificate	
	certificate of the CA	of the CA which issued the	
	which issued the	certificate	
.1	certificate	IZ 11 CC Cd 1	A1 1
authorityKeyIdentifier	Key identifier of the	Key identifier of the issuers	No change
	issuers public key corresponding to the	public key corresponding to the private key used to sign a	
	private key used to	certificate	
	sign a certificate	Continuate	
	10 %		

Version date: 20-03-2023	Version: 1.1	Page 5 of 12

subjectKeyIdentifier	Key identifier of the subject's public key included in the certificate	Key identifier of the subject's public key included in the certificate	No change
basicConstraints	cA: FALSE	cA: FALSE	No change
subjectAlternativeName	If present it includes the subjects e-mail address	If present it includes the subjects e-mail address	No change
qcStatement-2	Not present	semanticsIdentifier: semanticsIdentifier: id-etsi- qcs-semanticsId-Natural nameRegistrationAuthorities: https://uid.gov.dk	

 Version date: 20-03-2023
 Version: 1.1
 Page 6 of 12

3 VOCES (organizational certificates)

3.1 Certificate content

3.1.1 Formalia

Field	VOCES2	VOCES3 – VOCES profile	Remarks
X.509 version	3	3	No change ⁴
SerialNumber			No change
Validity Period			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with	RSASSA-PSS with SHA-	
	SHA-256	256 ⁵	
Trust anchor	TRUST2408	Den Danske Stat OCES	
		rod-CA	
Public key	2048 bits RSA key	3072 bits RSA key	

3.1.2 Distinguished Name

Field	VOCES2	VOCES3 – VOCES profile	Remarks
country	DK	DK	No change
organizationName	Certificate subscribers organizational name and CVR number (UTF8String) in the form "OrgName // CVR:xxxxxxxxx" where the OrgName is the registered name of the organization and xxxxxxxxx is the CVR number	Certificate subscribers organizational name	The separator ' // ' and the CVR-number is not included in organizational name in VOCES3. For VOCES3 the CVR can be found in organisationIdentifier
organizationalUnit	Optional	No supported	
commonName	organizations name optional organization unit names and optional function description		
organizationIdentifier	N/A	Certificate subscriber's CVR-number in the form NTRDK-XXXXXXXX where XXXXXXXXX is the CVR-number of the organization.	
serialNumber	Unique identifier for the certificate subject in the form CVR:XXXXXXXX-UID:XXXX	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Note that the X's in the MOCES3 is NOT the certificate subjects UID-number.

 $^{^{\}rm 5}$ Note that CA certificates are using SHA-512

Version date: 20-03-2023	Version: 1.1	Page 7 of 12
--------------------------	--------------	--------------

 $^{^{\}rm 4}$ Note that ASN.1-wise this value is encoded as the value 2 since X.509 enumerates from 0.

3.1.3 Extensions

Field	VOCES2	VOCES3 – VOCES profile	Remarks
keyUsage	contentCommitment,	digitalSignature,	VOCES3 use
	keyEncipherment,	contentCommitment,	profile F of ETSI
	dataEncipherment,	keyEncipherment	EN 319 412-2
	keyAgreement		section 4.3.2
certificatePolicies	OID reference to	OID references to VOCES3	The link to
	VOCES2 policies +	policies +	repository and
	Link to repository +	OID reference to the	the user notice is
	User notice	compliant NCP policy	discontinued
	referencing the		
	underlying policy.		
cRLDistributionPoints	HTTP link to CRL +	HTTP link to CRL	LDAP path to a
	LDAP path to a partial		partial CRL is
	CRL		discontinued
accessInformationAuthority	Reference to OCSP	Reference to OCSP	No change
	responder +	responder +	
	Reference to the	Reference to the certificate	
	certificate of the CA	of the CA which issued the	
	which issued the	certificate	
	certificate		
authorityKeyIdentifier	Key identifier of the	Key identifier of the issuers	No change
	issuers public key	public key corresponding to	
	corresponding to the	the private key used to sign a	
	private key used to	certificate	
	sign a certificate	Karridantifian af the ambient/a	No de ses
subjectKeyIdentifier	Key identifier of the	Key identifier of the subject's	No change
	subject's public key	public key included in the	
	included in the	certificate	
hasiaCanatusints	certificate	-A. FALSE	No shansa
basicConstraints subjectAlternativeName	cA: FALSE	cA: FALSE If present it includes the	No change
subjectAtternativeName	If present it includes	subjects e-mail address	No change
	the subjects e-mail	subjects e-man address	
qcStatement-2	address Not present	semanticsIdentifier:	
qostatement-2	Mot hieselit	semanticsIdentifier:	
		id-etsi-qcs-semanticsId-Legal	
		la con que semantiena Legar	
		nameRegistrationAuthorities:	
		https://uid.gov.dk	

Version date: 20-03-2023	Version: 1.1	Page 8 of 12

4 FOCES (Functional certificates)

Note that FOCES certificate policies are discontinued and in the OCES3 infrastructure FOCES is just a profile under the VOCES certificate policy.

4.1 Certificate content

4.1.1 Formalia

Field	FOCES2	VOCES3 – FOCES profile	Remarks
X.509 version	3	3	No change ⁶
SerialNumber			No change
Validity Period			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with	RSASSA-PSS with SHA-	
	SHA-256	256 ⁷	
Trust anchor	TRUST2408	Den Danske Stat OCES	
		rod-CA	
Public key	2048 bits RSA key	3072 bits RSA key	

4.1.2 Distinguished Name

Field	FOCES2	VOCES3 – FOCES profile	Remarks
country	DK	DK	No change
organizationName	Certificate subscribers organizational name and CVR number (UTF8String) in the form "OrgName // CVR:xxxxxxxxx" where the OrgName is the registered name of the organization and xxxxxxxxx is the CVR number	Certificate subscribers organizational name	The separator ' // ' and the CVR-number is not included in organizational name in VOCES3. For VOCES3 the CVR can be found in organisationIdentifier
organizationalUnit	Optional	No supported	
commonName	organizations name optional organization unit names and optional function description		
organizationIdentifier	N/A	Certificate subscriber's CVR-number in the form NTRDK-XXXXXXXX where XXXXXXXXX is the CVR-number of the organization.	
serialNumber	Unique identifier for the certificate subject in the form CVR:XXXXXXXX-UID:XXXX	Unique identifier for the certificate subject in the form UI:DK-X:X:XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	Note that the X's in the MOCES3 is NOT the certificate subjects UID-number.

 $^{^{\}rm 6}$ Note that ASN.1-wise this value is encoded as the value 2 since X.509 enumerates from 0.

 $^{^{\}rm 7}$ Note that CA certificates are using SHA-512

Version date: 20-03-2023	Version: 1.1	Page 9 of 12

4.1.3 Extensions

Field	FOCES2	VOCES3 – FOCES profile	Remarks
keyUsage	contentCommitment, keyEncipherment, dataEncipherment,	digitalSignature, keyEncipherment	VOCES3 use profile D of ETSI EN 319 412-2
	keyAgreement	015 () 1/00553	section 4.3.2
certificatePolicies	OID reference to	OID references to VOCES3	The link to
	VOCES2 policies +	policies +	repository and
	Link to repository + User notice	OID reference to the	the user notice is discontinued
		compliant NCP policy	discontinued
	referencing the		
cRLDistributionPoints	underlying policy. HTTP link to CRL +	HTTP link to CRL	LDAP path to a
CREDISTIBUTIONPOINTS	LDAP path to a partial	HTTP IIIK to CKL	partial CRL is
	CRL		discontinued
accessInformationAuthority	Reference to OCSP	Reference to OCSP	No change
accessifiormationAuthority	responder +	responder +	No change
	Reference to the	Reference to the certificate	
	certificate of the CA	of the CA which issued the	
	which issued the	certificate	
	certificate		
authorityKeyldentifier	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	Key identifier of the issuers public key corresponding to the private key used to sign a certificate	No change
subjectKeyIdentifier	Key identifier of the	Key identifier of the subject's	No change
	subject's public key included in the certificate	public key included in the certificate	
basicConstraints	cA: FALSE	cA: FALSE	No change
subjectAlternativeName	Not present	If present it includes the subjects e-mail address	No change
qcStatement-2	Not present	semanticsIdentifier: semanticsIdentifier: id-etsi-qcs-semanticsId-Legal	
		nameRegistrationAuthorities:	
		https://uid.gov.dk	

Version date: 20-03-2023	Version: 1.1	Page 10 of 12
İ	l l	J

5 CRL

5.1 CRL content

5.1.1 Formalia

Field	OCES2	OCES3	Remarks
X.509 version	2	2	No change ⁸
SerialNumber			No change
thisUpdate			No change
nextUpdate			No change
Signature algorithm	RSASSA-PKCS1-v1_5 with	RSASSA-PSS with SHA-	
	SHA-256	512	
Trust anchor	TRUST2408	Den Danske Stat OCES	
		rod-CA	

5.1.2 Extensions

Field	OCES2	OCES3	Remarks
CRL Number			No change
authorityKeyIdentifier	Key identifier of the issuers public key corresponding to the private key used to sign	Key identifier of the issuers public key corresponding to the private key used to sign	No change
	a certificate	a certificate	
expiredCertificatesOnCRL	Not present	The inclusion of this extension indicates that the revocation information contains information about revoked certificates since the date described in the time.	

⁸ Note that ASN.1-wise this value is encoded as the value 1 since X.509 enumerates from 0.

Version date: 20-03-2023	Version: 1.1	Page 11 of 12

6 More information

The full specification of OCES3 certificates and CRL can be found at the repository of the OCES3 trust provider "Den Danske Stat" at https://ca1.gov.dk.

 Version date: 20-03-2023
 Version: 1.1
 Page 12 of 12